PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/06 — A1

(11) International Publication Number: WO 00/41356

(43) International Publication Date: 13 July 2000 (13.07.00)

(21) International Application Number: PCT/EP99/10208

(22) International Filing Date: 16 December 1999 (16.12.99)

(30) Priority Data:

1010921	30 December 1998 (30.12.98)	NL
1011544	12 March 1999 (12.03.99)	NL
1011800	15 April 1999 (15.04.99)	NL

(71) Applicant *(for all designated States except US)*: KONINKLIJKE KPN N.V. [NL/NL]; Stationsplein 7, NL–9726 AE Groningen (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: ROELOFSEN, Gerrit [NL/NL]; Rijndijk 60–A, NL–2331 AH Leiden (NL). VAN BRUCHEM, Dirk, Jan, Jacobus [NL/NL]; Randveen 4, NL–2291 NM Wateringen (NL). MULLER, Frank [NL/NL]; Meerkoetlaan 24, NL–2623 NJ Delft (NL). ROMBAUT, Willem [NL/NL]; C.A. van Beverenplein 11, NL–2552 HT Den Haag (NL).

(74) Agent: KLEIN, Bart; Koninklijke KPN N.V., P.O. Box 95321, NL–2509 CH The Hague (NL).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

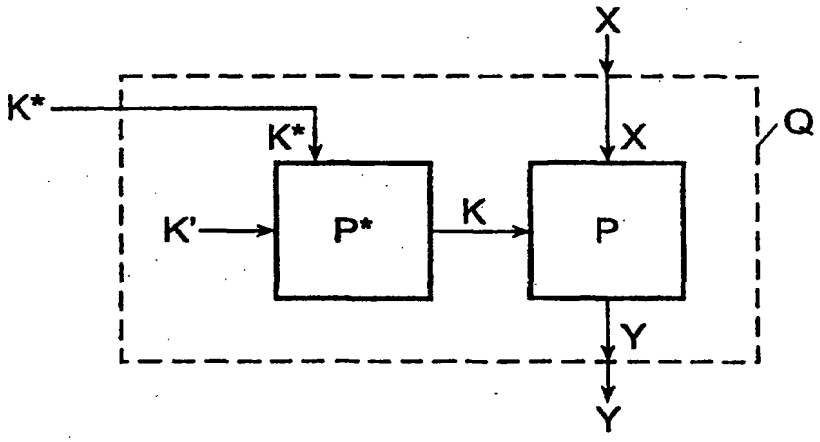
Published

With international search report.

(54) Title: METHOD AND DEVICE FOR CRYPTOGRAPHICALLY PROCESSING DATA

(57) Abstract

In the event of cryptographically processing data, said data (X) and a key (K) are fed to a cryptographic process (P), which may be a known process. In order to veil the nature of the process (P), there are fed auxiliary values to the process, such as a supplementary key (K*), using which a supplementary process (P*) generates the key proper (K). The combination of the original process (P) and the supplementary process (P*) provides an unknown process, the relationship between the supplementary key (K*) and the processed data (Y) being unknown. As a result, there is obtained an improved cryptographic security.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Method and device for cryptographically processing data.

BACKGROUND OF THE INVENTION

The invention relates to a method for cryptographically processing data, comprising feeding, to a cryptographic process, values, namely, the data and a key, and carrying out the process in order to form cryptographically processed data. Such method is generally known.

For cryptographically processing data, in practice there are often applied generally known processes. Examples of such cryptographic processes (algorithms) are DES and RSA [DES = Data Encryption Standard and RSA = Rivest, Shamir & Adleman], which are described, e.g., in the book "Applied Cryptography" by B. Schneier (2nd edition), New York, 1996.

Said processes are published since it was assumed that, in the event of sufficiently large key lengths, it would be impossible, on the basis of the processed data, to retrieve the original data and/or the key, even if the cryptographic process were known.

Recently, however, there were discovered attacks which are based on knowledge of the cryptographic process. In other words, since the behaviour of the process is known, in the event of certain attacks it becomes considerably more simple to derive the key used and/or the original data. It will be understood that such is undesirable.

SUMMARY OF THE INVENTION

The object of the invention is to solve the above problem by indicating a method and circuit, for carrying out a cryptographic process, which render the derivation of the key in the event of application of a known (i.e., public) cryptographic process considerably more difficult or even impossible. For this purpose, a method of the type referred to in the preamble according to the invention is characterised by feeding, to the process, auxiliary values in order to mask the values used in the process.

By masking the date and/or key(s) it becomes considerably more difficult to derive said values on the basis of the behaviour of the process. The result of the process, i.e., the collection of processed data, in the event of a suitable choice of the auxiliary values may be unchanged, i.e., identical to the result of the process, if no auxiliary values have been fed to it. In this connection, an "auxiliary value" is understood to

mean a value (data or key) which is fed to the process as a supplement to the corresponding data and key.
The invention is therefore based on the insight that the derivation of the values used in a cryptographic process is rendered considerably more difficult if said values are masked using auxiliary values.

The invention is partly based on the further insight that the use of auxiliary values does not necessarily affect the outcome of the process.

In a first embodiment of the invention, an auxiliary value comprises a supplementary key which is fed to a supplementary process in order to form the key.

By applying a combination of a known process and a supplementary process, there is formed a new cryptographic process, unknown per se, even if the supplementary process is also known per se.

By deriving the key used for the known process (primary key) from a supplementary key (secondary key) using a supplementary process, there is achieved that not the (primary) key of the known process but the supplementary (secondary) key is offered to the combination of processes. In other words, externally the supplementary (secondary) key, and not the real (primary) key of the process proper, is used. Derivation of the key from the original data and the processed data has thereby become impossible. In addition, the derivation of the supplementary key has been rendered seriously more difficult, since the combination of the original process and the supplementary process is not known.

Said embodiment of the invention is therefore based, inter alia, on the insight that the being known of a cryptographic process is undesirable, such contrary to what was so far assumed. Said embodiment is also based on the further insight that attacks which elaborate on knowledge of the process become considerably more difficult if the process is unknown.

The supplementary process preferably comprises a cryptographic process. This renders the derivation of the supplementary key more difficult. Basically, however, a simple encoding may be applied, e.g., as a supplementary process. In the event of a cryptographic process, there is preferably applied an auxiliary key.

The supplementary process advantageously is an invertible process. This enables the application of the method according to the invention in existing equipment with minimum modifications.

If, e.g., a first device gives off a (supplementary) key which is applied in a second device according to the invention, then in the first device there may be used the inverse of the supplementary process to derive the supplementary key from the original key. In other words, although in both the first and the second device internally the original (primary) key is used, there is exchanged, between the devices, the supplementary (secondary) key. Intercepting the supplementary key, however, does not result in knowledge of the original key.

It may be advantageous if carrying out the supplementary process takes place exclusively if the data has predetermined properties. In this manner, cryptographic processing may be carried out for specific, selected data only, while such is blocked for all other data. In this manner, there is achieved a supplementary protection.

An optimum security is provided if the process and the supplementary process are each constructed of several steps and in which there are alternately carried out steps of the process and the supplementary process. As a result, the properties of the known process are further veiled, as a result of which the derivation of the keys is further complicated.

In a second embodiment of the invention, the process comprises several steps, each of which has a cryptographic operation for processing right-hand data derived from the data and a combinatory operation for combining, with the left-hand data derived from the data, the processed right-hand data in order to form modified left-hand data, in which the right-hand data, prior to the first step, is combined with a primary auxiliary value and the left-hand data is combined with an additional auxiliary value. As a result, the data used in the steps and transferred between the steps is masked.

In order to make it possible for the primary and additional auxiliary values do not make themselves felt in the end result of the process, the right-hand data is combined, preferably immediately after the last step, with a further primary auxiliary value, and the modified left-hand data is combined with a further additional auxiliary value.

In order not to have the result of the operations affected by the primary auxiliary values, the method according to the invention is preferably carried out in such a manner that the right-hand data, in each step and prior to the operation, is combined with the primary auxiliary value of said step.

A further protection is achieved if the processed right-hand data, following the processing, is combined with a secondary auxiliary value of said step.

The secondary auxiliary value of a step is advantageously formed from the combination of the primary auxiliary value of the preceding step and the primary auxiliary value of the next step. As a result, it becomes possible to compensate the auxiliary value in the repeatedly next step, as a result of which said auxiliary value will not make itself felt in the end result of the process.

It is possible to carry out the method according to the invention in such a manner, that all primary auxiliary values are equal. As a result, a very simple practical realisation is possible. The use of several auxiliary values, which are preferably random numbers and are generated anew for each time the process is carried out, however, offers a greater cryptographic security.

A further simplification of said embodiment may be obtained if the primary auxiliary values and/or secondary auxiliary values repeatedly have been combined in advance with the operation in question. This is to say, combining with auxiliary values is processed in the operation in question (e.g., a substitution), in such a manner that the result of the operation in question is equal to that of the original operation plus one or two combinatory operations with auxiliary values. By in advance including in the operation the combinatory operations, a more simple and faster practical realisation is possible.

Said combinatory operations are preferably carried out using an XOR operation [XOR = eXclusive OR]. Other combinatory operations, however, such as binary adding, are basically possible as well.

The invention further provides a circuit for carrying out a method for cryptographically processing data. In addition, the invention supplies a payment card and a payment terminal provided with such circuit.

Below, the invention will be further explained on the basis of the exemplary embodiments shown in the figures.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 schematically shows a cryptographic process according to the prior art.

FIG. 2 schematically shows a first cryptographic process according to a first embodiment of the invention.

FIG. 3 schematically shows a second cryptographic process according to a first embodiment of the invention.

FIG. 4 schematically shows a way in which the processes of figures FIG. 1 and 2 may be carried out.

FIG. 5 schematically shows a cryptographic process having several steps according to the prior art.

FIG. 6 schematically shows a first cryptographic process according to a second embodiment of the invention.

FIG. 7 schematically shows a second cryptographic process according to a second embodiment of the invention.

FIG. 8 schematically shows a third cryptographic process according to a second embodiment of the invention.

FIG. 9 schematically shows a circuit in which the invention is applied.

FIG. 10 schematically shows a payment system in which the invention is applied.

PREFERRED EMBODIMENTS

A (cryptographic) process P according to the prior art is schematically shown in FIG. 1. To the process P, there are fed input data X and a key K. On the basis of the key K, the process P converts the input data X into (cryptographically) processed output data Y: $Y = P_K(X)$. The process P may be a known cryptographic process, such as DES (Data Encryption Standard), triple DES, or RSA (Rivest, Shamir & Adleman).

If the input data X and the output data Y are known, it is basically possible to derive the key K used. In the event of a key of sufficient length (i.e., a sufficient number of bits), it was so far deemed impossible to derive said key, even if the process P were known. Impossible in this case is to say that in theory it is admittedly possible, e.g., by trying out all possible keys, to retrieve the key used, but that such requires an impossibly long computational time. Such "brute-force attack" is therefore hardly a threat to the cryptographic security.

Attacks recently discovered, however, make use of knowledge of the process, as a result of which the number of possible keys may be reduced drastically. Deriving the key K used and/or the input data X from the output data Y therefore becomes possible within acceptable computational times.

The principle of the invention, whose object it is to render such attacks considerably more difficult and time-

consuming, is schematically shown in FIG. 2. Just as in FIG. 1, to a (known) process P there are fed input data X and a (secret) key K to generate output data Y.

Contrary to the situation of FIG. 1, in the situation of FIG. 2 the key K is fed to the process P from a supplementary process P*. The supplementary process P* has a supplementary (secondary) key K* as input data to produce, under the influence of an auxiliary key K', the (primary) key K as output data. The key K is therefore not fed, as is the case in the situation of FIG. 1, from an external source (e.g., a memory) to the process P, but is produced by the process P* from the supplementary (secondary) key K*:

$$K = P^*_{K'}(K).$$

It is therefore the secondary key K*, instead of the primary key K, which is predetermined and stored, e.g., in a key memory (not shown). According to the invention, the primary key K, which is fed to the process P, is not predetermined.

The auxiliary key K' may be a permanently stored, predetermined key. It is also possible to apply a supplementary process P* in which no auxiliary key K' is used.

The combination of the processes P and P* forms a new process which is schematically designated by Q. To the process Q which, on account of the supplementary process P*, is unknown per se, the input data X and the (secondary) key K* are fed to produce the output data Y. The relationship between the secondary key K* and the primary key K is veiled by the supplementary process P*.

The supplementary process P* preferably is the inverse of another, invertible process R. This is to say:

$$P^* = R^{-1}.$$

This enables producing the secondary key K* from the primary key K using R and the auxiliary key K':

$$K^* = R_{K'}(K),$$

as will be further explained later by reference to FIG. 5. The new process Q may possibly be extended by the process R, in such a manner that the primary key K, instead of the s condary key K*,

is fed to the process Q. The primary key K in this case in the process Q is derived from:

$$K = P^*_{K'}(K^*) = P^*_{K'}(R_{K'}(K)).$$

This enables using the same (primary) key as in the prior art.

The cryptographic process Q according to the invention, schematically shown in FIG. 3, also comprises a process P having a primary key K and a supplementary process P* having an auxiliary key K', the primary key K being derived from the supplementary key K* by the supplementary process P*. Supplementing the process of FIG. 1, in this case the input data X is also fed to the supplementary process P*, in such a manner that the primary key K is determined partly as a function of the input data X:

$$K = P^*_{K'}(K^*, X).$$

As a result, there is obtained a supplementary cryptographic protection. In addition, as a result the possibility is offered to carry out the supplementary process P* exclusively if certain input data is offered. This is to say that the supplementary process P* may comprise a test of the input data X, and carrying out the supplementary process P* may depend on the result of said test. Thus, the supplementary process P*, e.g., may be carried out only if the last two bits of the input data X equal zero. The effect of such an input data-dependent operation is that only for certain input data X the correct primary key K will be produced in such a manner that only said input data will deliver the desired output data Y. It will be understood that as a result the cryptographic security is further enhanced.

FIG. 4 schematically shows the way in which substeps of the processes P and P* may be carried out alternatingly ("interleaving") in order to further enhance the protection against attacks. The substeps may include so-called "rounds", such as, e.g., in the case of DES. The substeps, however, preferably comprise only one or a few instructions of a program, with which the processes are being carried out.

In a first step 101, there is carried out a first substep P_1 of the process P. Subsequently, in a second step 102, the first substep P_1* of the supplementary process P* is carried out.

Likewise, in a third step 103, the second substep P_2 of the process P is carried out etc. This continues until, in step 110, the last substep P_n^* of the supplementary process P* has been carried out, it being assumed, for the sake of the example, that the processes P and P* comprise an equal number of substeps. If such is not the case, in step 110 there is carried out the last corresponding substep, and in further steps the remaining substeps are carried out.

By alternating the substeps of the process P, which is known per se, and the process P* (possibly known per se as well), there may be obtained a series of substeps which does not correspond to that of a known process. As a result, the nature of the process is more difficult to recognise.

The cryptographic process P schematically shown, only by way of example, in FIG. 5, according to the prior art comprises several steps S_i (i.e., S_1, S_2, ..., S_n). In each step S_i, (right-hand) data RD_i is fed to a cryptographic operation F_i. Said cryptographic operation may itself comprise a number of substeps, such as an expansion, a combination with a key, a substitution and a permutation which, however, have not been designated separately for the sake of the simplicity of the drawing. The cryptographic operation F_i provides processed data FD_i:

$$FD_i = F_i(RD_i).$$

In a combinatory operation CC_i (CC_1, CC_2, ..., the index i always indicating the step S in question), the processed data FD_i is combined with left-hand data LD_i to form modified (left-hand) data SD_i which, just as the original right-hand data RD, is passed on to the next step. The combinatory operations CC_i preferably are XOR operations (symbol: $\oplus$).

As is shown in FIG. 5, at the end of each step S_i the modified left-hand data SD_i and the right-hand data RD_i change positions in such a manner that they form the right-hand data RD_{i+1} and the left-hand data LD_{i+1} of the next step S_{i+1}.

The left-hand data LD_1 and the right-hand data RD_1 of the first step S_1 were derived, in a preceding operation, from input data X and, in doing so, may undergo a preparatory processing, such as an input permutation. The output data SD_n and RD_n of the last step S_n form the processed data Y of the proces P, possibly after it has undergone a final operation, such as an output permutation PP^{-1}.

The cryptographic process of FIG. 6 largely corresponds to that of FIG. 5. In accordance with the invention, the data present in and between the steps is masked with auxiliary values. For this purpose, in this embodiment the first step S_1 is preceded by (preparatory) combinatory operations DC and EC, which are preferably XOR operations as well. They combine the left-hand data LD_1 and the right-hand data RD_1, respectively, which originate from the preparatory operation (PP), with a zeroth auxiliary value A_0 and a first auxiliary value A_1. The results of the combinatory operations DC and EC are left-hand masked data LD'_1 and right-hand masked data RD_1', respectively (*in the continuation of this text, masked data will be designated by an apostrophy*). The maskings make themselves felt in the subsequent steps. Since the left-hand data of the second step S_2 is equal to the masked right-hand data of the first step S_1, said left-hand data LD'_2 is masked as well. The right-hand data RD_2' of the second step is masked since it is equal to the masked, modified data SD_1'.

Combining the data LD_i and RD_i with the auxiliary values A_i therefore results in the modified data LD_i' and RD_i' being masked, as a result of which it is considerably more difficult to derive the original data X or the key used from the masked data LD_i' and RD_i'.

In order to remove the auxiliary values A_i prior to the final operation (PP^{-1}), there are provided completing combinatory operations FC and GC, which combine the modified and masked left-hand data SD'_n of the last step S_n with an auxiliary value A_{n+1} and the masked right-hand data RD_n' with an auxiliary value A_n, respectively. On account of $A_i \oplus A_i$ being zero in this manner the maskings are removed by the auxiliary values A_i. As a result, it is possible to carry out the method in such a manner that, notwithstanding the use of the auxiliary values A_i, the final data Y is equal to that which would have been obtained by the conventional method according to FIG. 5.

In order to exclude the effect of the auxiliary values A_i on the results FD_i of the operations F_i, in each step S_i there is preferably present a supplementary combinatory operation AC_i which combines the right-hand data RD_i with a (primary) auxiliary value A_i before this data is fed to the cryptographic operation F_i. The result of each supplementary combinatory operation AC_i is non-masked right-hand data RD_i, so that the cryptographic operation F_i works on the same data as in the process of FIG. 5.

There may be advantageously inserted a further combinatory operation BC_i between the cryptographic operation F_i and the combinatory operation CC_i with the purpose of combining the processed (right-hand) data FD_i with a further (secondary) auxiliary value B_i. As a result, there may be achieved a masking of the processed data FD_i and a further masking of the (modified) left-hand data SD_i'. The combinatory operations AC_i and BC_i preferably are XOR operations as well.

In accordance with a further aspect of the invention, the auxiliary values A_i and B_i are related. The secondary auxiliary values B_i are formed, preferably using an XOR operation, from the first auxiliary value A_{i-1} of the previous step and the auxiliary value A_{i+1} of the next step:

$$B_i = A_{i-1} \oplus A_{i+1}.$$

This results in each primary auxiliary value A_{i+1} which, using a further supplementary combinatory operation BC_i, is combined with the processed right-hand data FD_i as an ingredient of the secondary auxiliary value B_i, repeatedly being compensated in the next step, i.e., step S_{i+1}, by means of a combinatory operation AC_i before the right-hand data RD_{i+1} is subjected to the operation F_i. The (masked) right-hand data RD_i' in question, which forms the (masked) left-hand data LD_{i+1}' of the still next step S_{i+2} are combined there with the primary auxiliary value A_{i+1} and is compensated in this manner. The auxiliary value A_{i+1} makes itself felt in the modified data SD_i', in such a manner that this remains masked between two steps.

The left-hand data LD_1 of the first step S_1 is masked with the additional or zeroth (primary) auxiliary value A_0. By combining, with the secondary auxiliary value $B_1 = A_0 \oplus A_2$, the initial auxiliary value A_0 is removed (on account of $A_0 \oplus A_0$ being zero), but the auxiliary value A_2 and the masking achieved therewith are maintained. The zeroth auxiliary value A_0 in this embodiment is preferably chosen equal to the first auxiliary value A_1.

Although all primary auxiliary values A_i are preferably chosen different, with the exception of $A_0 = A_1$, it is possible to choose all primary auxiliary values A_i equal. In this case, all secondary auxiliary values B_i in the embodiment shown will be equal to zero, so that the further combinatory operations BC_i may be omitted. The invention further applies to processes P which contain only one step S, or have a deviating structure.

In the process of FIG. 7, which largely corresponds to that of FIG. 6, the combinatory operations AC_i and BC_i and the cryptographic operation F_i in each step are integrated to form a combined operation F_i'. Integrating the combinatory operations in the operations F_i is possible by suitably adjusting, e.g., a substitution table of the operation F_i. As a result, the supplementary combinatory operations AC_i and BC_i may be omitted and the result of the adjusted operation F_i' is equal to the result of the total of the operation F_i proper and the combinatory operations:

$$FD_i' = F_i'(RD_i') = B_i \oplus F_i (A_i \oplus RD_i').$$

Basically, each step S_i requires a different combinatory operation F_i in which various auxiliary values A_i are integrated (see FIG. 6). Only if the auxiliary values A_i are chosen equal, i.e., $A_1=A_2 = \ldots = A_n$, the combinatory operations F_i in this embodiment may be equal.

Each time the process is carried out, the values A_i are preferably chosen anew. For the process of FIG. 7, this means that the combined operations F_i' are then determined anew. Since the operations F_i' in many implementations will comprise the use of several tables, such as substitution tables, said tables will be determined anew each time the process P is carried out. In order to offer a supplementary protection against attacks, according to a further aspect of the invention the tables will be determined in random order. If a combined operation F_i' comprises, e.g., eight tables, said eight tables will be determined in another order each time said operation F_i' is carried out anew. Said order may be determined on the basis of the contents of an order register, which contents may each time be formed by a random number originating from a random-number generator. On the basis of the contents of the order register there may each time be composed a fresh lookup table. Using the lookup table, the tables may be written to a memory and later be read out.

According to a further aspect of the invention, supplementing this or instead thereof, the elements of each table may be determined and/or stored in random order. With this measure it is achieved that the protection against attacks is also improved. In this case, too, there may be applied a lookup table on the basis of which the elements may later be retrieved.

The measures referred to above may also be applied in another embodiment of the invention, such as the one of FIG. 8,

or in completely different other processes, whether cryptographic or not.

The embodiment of FIG. 8 largely corresponds to that of FIG. 7. Supplementing FIG. 7, each step S_i, with the exception of the last step S_n, includes a combinatory operation HC_i which combines the right-hand data RD_i with a tertiary auxiliary value W_i. The tertiary auxiliary value W_i preferably equals the XOR combination of the auxiliary values A_0 and A_1:

$$W = A_0 \oplus A_1,$$

where $A_0 \neq A_1$.

This results in the operation HC_i always adding the zeroth auxiliary value A_0 and compensating the first auxiliary value A_1. As a result, it is possible that all cryptographic operations F_i are essentially identical, which requires a much smaller processing and/or storage capacity from a processor system with which the method is carried out. In the embodiment of FIG. 8, the operations F_i" are such adjustments of the original operations F_i, that these are corrected for the auxiliary value A_1 and in addition combine the tertiary auxiliary value $W = A_0 \oplus A_1$ with their result. In other words, if $RD_i \oplus A_1$ is fed to F", the result will be equal to

$FD_i' = F_i(RD_i) \oplus W$.

It will be understood by those skilled in the art that the combinatory processes AC_i, BC_i and HC_i may be carried out in different locations in the cryptographic process P to achieve a comparable or even identical effect.

FIG. 9 schematically shows a circuit 10 for implementing the method according to the invention. The circuit 10 comprises a first memory 11, a second memory 12 and a processor 13, the memories 11 and 12 and the processor 13 being coupled using a data bus 14. By providing two memories, it is possible each time to carry out a substep of one of the processes P and P* (see FIG. 4), to store the result of said substep in, e.g., the first memory 11, and from the second memory 12 to transfer a previous interim result from the other process to the processor 13. In this manner, it is possible to efficiently carry out the alternating computation of substeps of two different processes.

The payment system schematically shown in FIG. 10 comprises an electronic payment means 1 and a payment station 2. The electronic payment means 1 is, e.g., a so-called smart card,

i.e., a card provided with an integrated circuit for storing and processing payment data. The payment station 2 comprises a card reader 21 and a processor circuit 22. The processor circuit 22 may correspond to the circuit 10 of FIG. 9.

At the beginning of a transaction, the payment means 1 transmits an identification (card identification) ID to the payment station 2. By reference to said identification, the payment station 2 determines a key which will be used for said transaction. Said identification ID may be fed as input data X (see the figures 1-3) to a cryptographic process which, on the basis of a master key MK, produces an identification-dependent transaction key K_{ID} as output data Y. In accordance with the invention, for this purpose the process shown in the figures FIG. 2 and 3 is used, the master key MK having been converted in advance, using a process R, into a supplementary master key MK*. Said supplementary master key MK* is now fed, preferably together with the identification ID, in accordance with FIG. 3, to the supplementary process P* in order to reproduce the original master key MK and to derive the transaction key K_{ID} from the identification ID.

Although, in the figures FIG. 2 and 3, there is always shown one single supplementary process P*, there may possibly be used several processes P*, P**, P***, ... in series and/or in parallel to derive the primary key K.

It will be understood by those skilled in the art that many modifications and amendments are possible without departing from the scope of the invention.

CLAIMS

1. Method for cryptographically processing data, comprising feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K), and carrying out the process (P) in order to form cryptographically processed data (Y), characterised by feeding, to the process (P), auxiliary values (K*; A, B) in order to mask the values (K; D) used in the process (P).

2. Method according to claim 1, wherein an auxiliary value comprises a supplementary key (K*) which is fed to a supplementary process (P*) in order to form the key (K).

3. Method according to claim 2, wherein the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed.

4. Method according to claim 2 or 3, wherein the supplementary process (P*) is an invertible process.

5. Method according to claim 2, 3 or 4, wherein the data (X) is also fed to the supplementary process (P*).

6. Method according to claim 5, wherein carrying out the supplementary process (P*) takes place exclusively if the data (X) has predetermined properties.

7. Method according to any of the claims 2-6, wherein the process (P) and the supplementary process (P*) each are built up from a number of steps, and wherein steps of the process (P) and the supplementary process (P*) are alternated.

8. Method according to any of the preceding claims, wherein the process (P) comprises a number of steps (S_i), each having a cryptographic operation (F_i, F_i', F_i'') for processing right-hand data (RD_i) derived from the data (X) and a combinatory operation (C_i) for combining with left-hand data (LD_i) also derived from the data (X), the processed right-hand data (FD_i) in order to form modified left data (SD_i), and wherein the right-hand data (RD_1) is combined with a primary auxiliary value (A_1) prior to the first step (S_1) and the left-hand data (LD_1) is combined with an additional auxiliary value (A_0).

9. Method according to claim 8 wherein, immediately after the last step (S_n), the right-hand data (RD_n) is combined with a further primary auxiliary value (A_n) and the modified left-hand data (SD_n') is combined with a further additional auxiliary value (A_{n+1}).

10. Method according to claim 8 or 9, wherein the right-hand data (RD_i) is combined, in each step (S_i) and prior to the operation (F_i'), with the primary auxiliary value (A_i) of said step (S_i).

11. Method according to claim 10, wherein the processed right-hand data (FD_i) is combined, following the operation (F_i), with the secondary auxiliary value (B_i) of said step (S_i).

12. Method according to claims 10 and 11, wherein the secondary auxiliary value (B_i) of a step (S_i) is formed from the combination of the primary auxiliary value (A_{i-1}) of the preceding step and the primary auxiliary value (A_{i+1}) of the next step.

13. Method according to any of the claims 8-12, wherein all primary auxiliary values (A_i) are equal.

14. Method according to any of the claims 9-13, wherein the primary auxiliary values (A_i) and/or secondary auxiliary values (B_i) have each time been combined with the respective operation (F_i) in advance.

15. Method according to claim 14, wherein a combined operation (F_i') contains several tables, and wherein the tables are determined in a different order each time the process (P) is carried out.

16. Method according to claim 14 or 15, wherein a combined operation (F_i') contains several tables, and wherein the elements of the tables are determined and/or stored in a different order each time the process (P) is carried out.

17. Method according to claim 16, wherein the order is stored as a lookup table for the benefit of reading out the elements.

18. Method according to any of the claims 8-17, wherein the right-hand data (RD_i) is combined with a tertiary auxiliary value (W_i) after each step (S_i).

19. Method according to claim 18, wherein the tertiary auxiliary value (W_i) in all steps, except the last one (S_n) is equal to the combination of the primary auxiliary value (A_1) of the first step (S_1) and the additional auxiliary value (A_0), and in the last step (S_n) is equal to zero.

20. Method according to any of the claims 8-19, wherein combining is carried out using an XOR operation.

21. Method according to any of the preceding claims, wherein the data (X) comprises identification data of a payment means (1) and the processed data (Y) forms a diversified key.

22. Method according to any of the preceding claims, wherein the process (P) comprises DES, preferably triple DES.

23. Circuit (10) for carrying out the method according to any of the preceding claims.

24. Payment card (1), provided with a circuit (10) according to claim 23.

25. Payment terminal (2) provided with a circuit (10) according to claim 23.

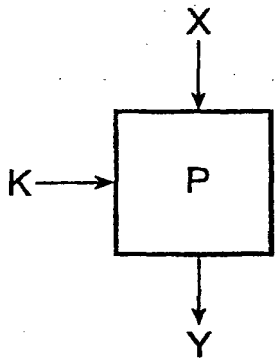


FIG. 1

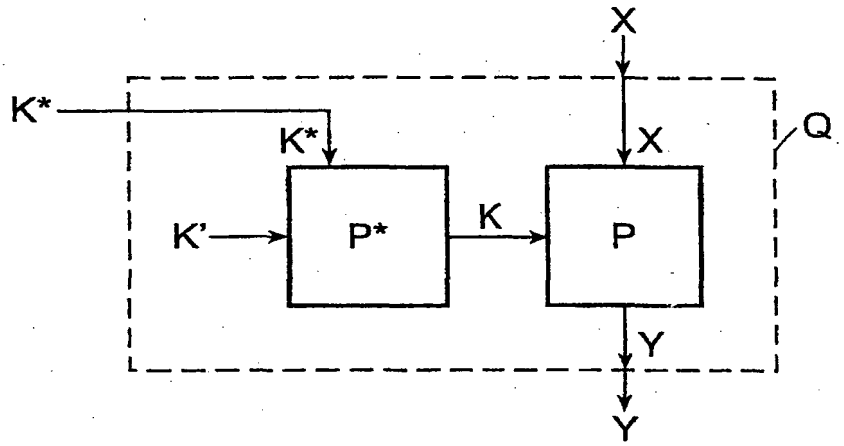


FIG. 2

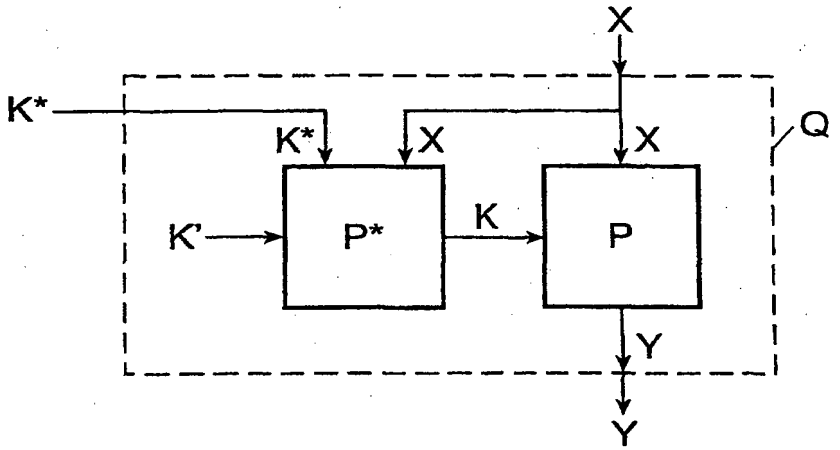


FIG. 3

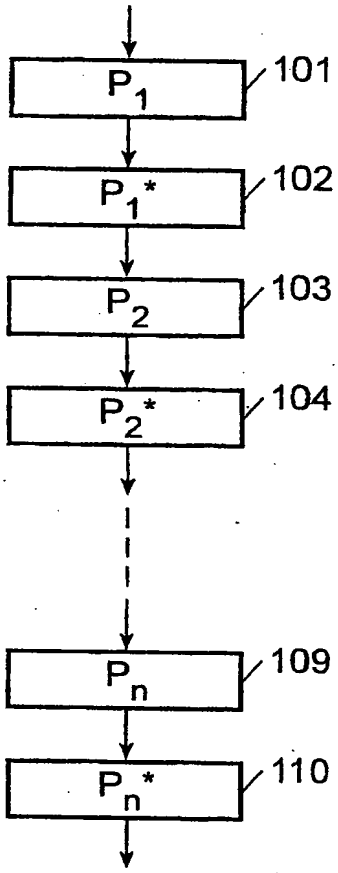


FIG. 4

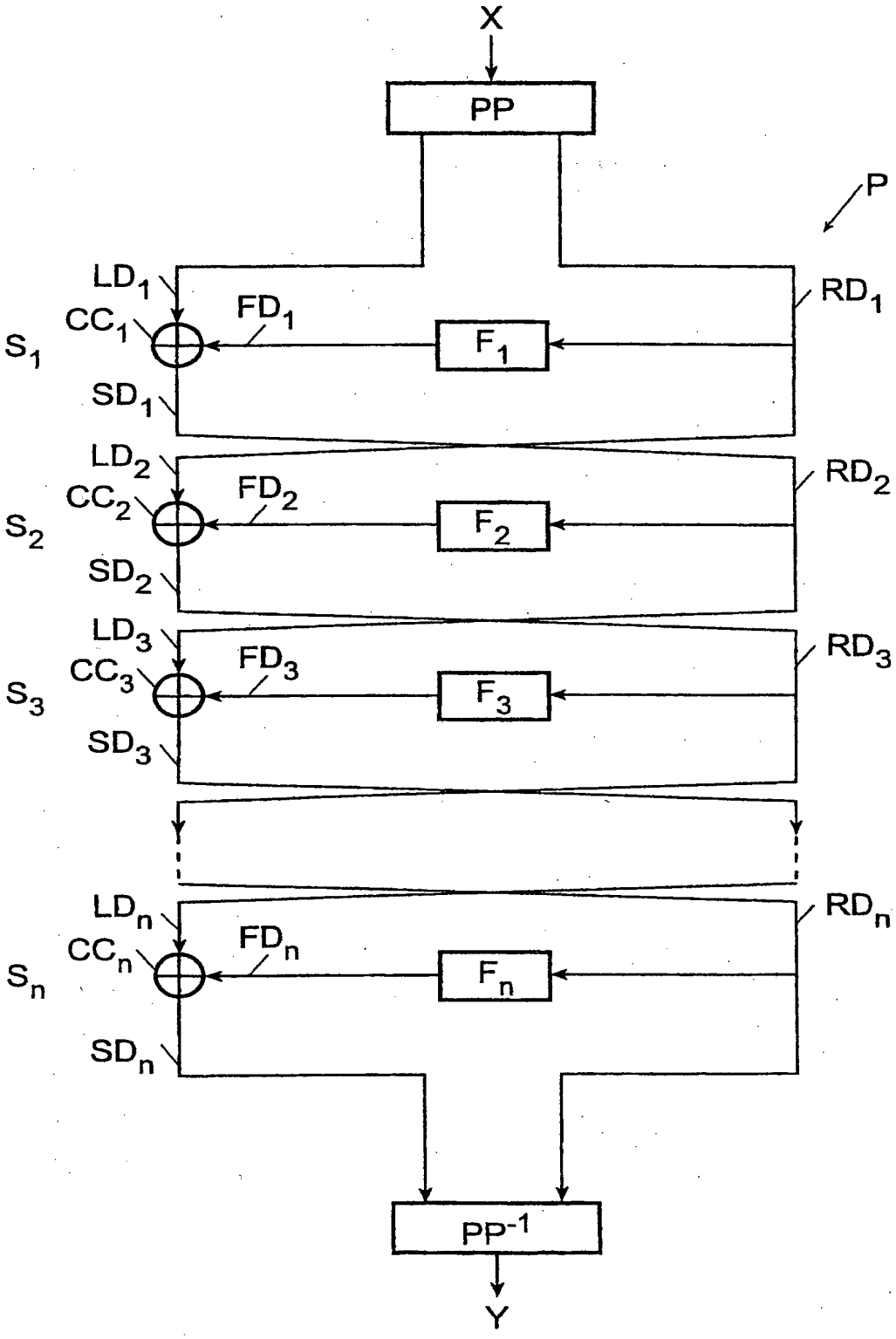

X
PP
P
LD1
CC1
FD1
F1
RD1
S1
SD1
LD2
CC2
FD2
F2
RD2
S2
SD2
LD3
CC3
FD3
F3
RD3
S3
SD3
LDn
CCn
FDn
Fn
RDn
Sn
SDn
PP-1
Y

FIG. 5

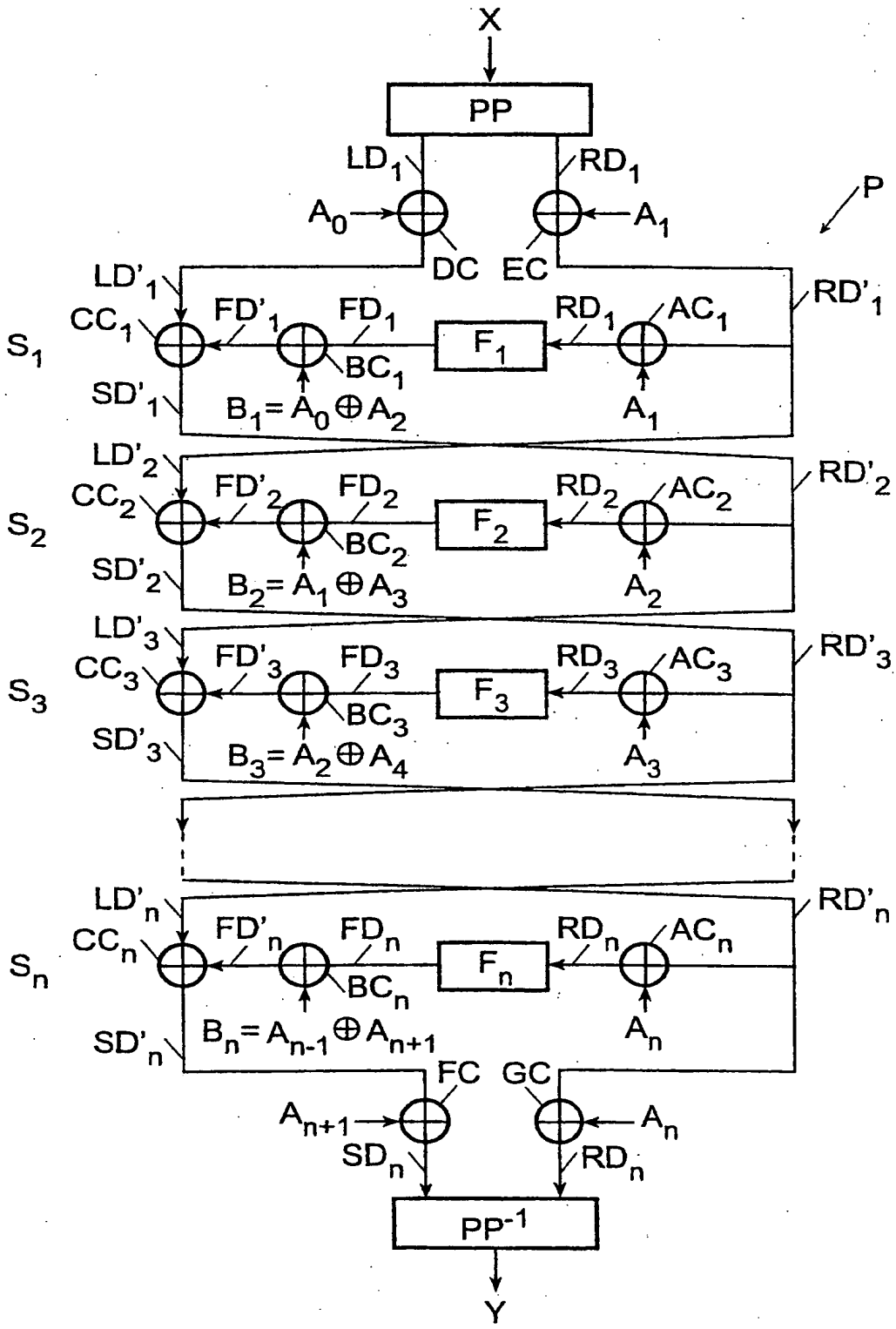

X
PP
LD1
RD1
A0
A1
P
DC
EC
LD'1
RD'1
CC1
FD'1
FD1
RD1
AC1
S1
F1
BC1
SD'1
B1= A0 ⊕ A2
A1
LD'2
RD'2
CC2
FD'2
FD2
RD2
AC2
S2
F2
BC2
SD'2
B2= A1 ⊕ A3
A2
LD'3
RD'3
CC3
FD'3
FD3
RD3
AC3
S3
F3
BC3
SD'3
B3= A2 ⊕ A4
A3
LD'n
RD'n
CCn
FD'n
FDn
RDn
ACn
Sn
Fn
BCn
SD'n
Bn= An-1 ⊕ An+1
An
FC
GC
An+1
An
SDn
RDn
PP-1
Y

FIG. 6

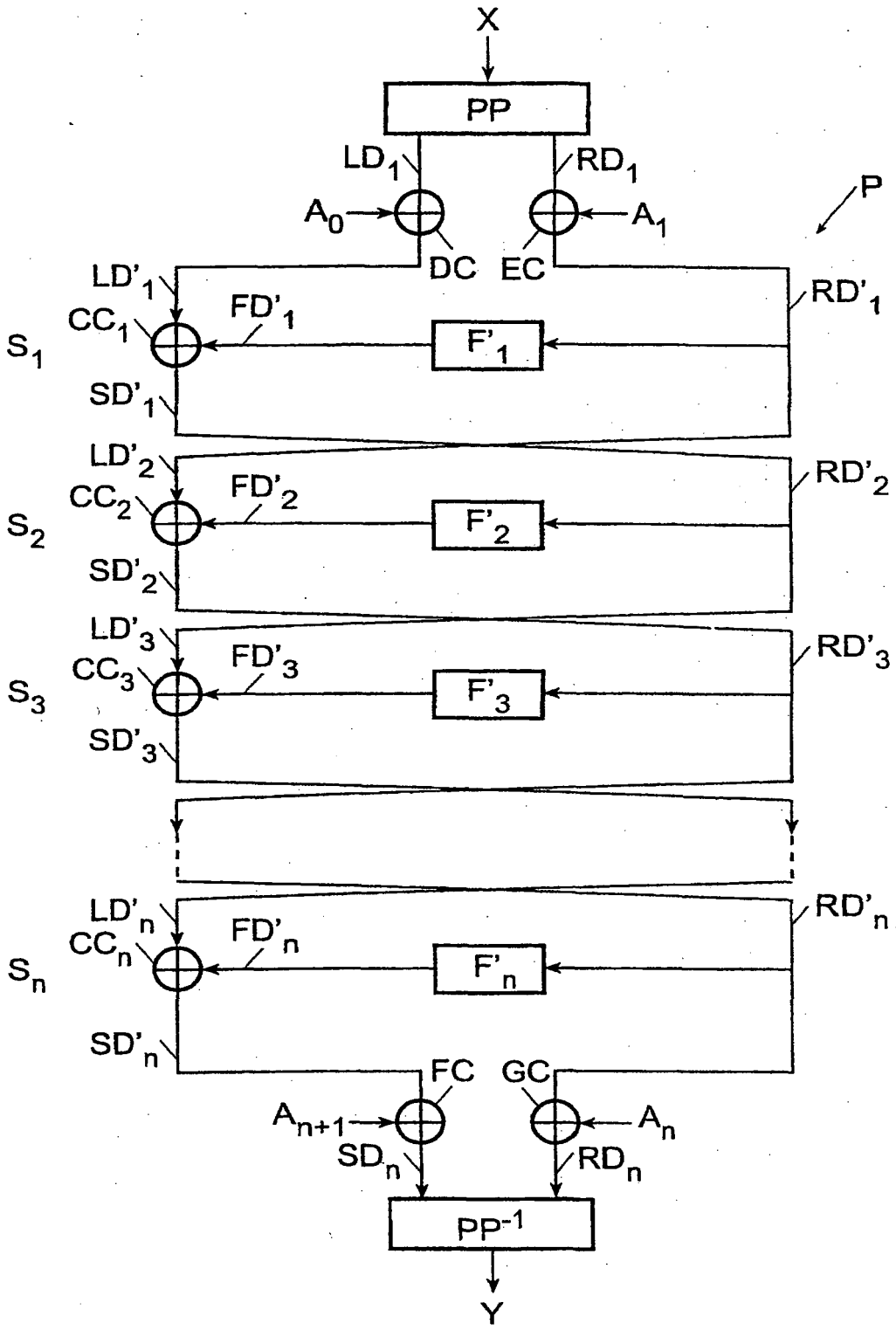

X
PP
LD1
RD1
A0
A1
P
DC
EC
LD'1
RD'1
CC1
FD'1
F'1
S1
SD'1
LD'2
RD'2
CC2
FD'2
F'2
S2
SD'2
LD'3
RD'3
CC3
FD'3
F'3
S3
SD'3
LD'n
RD'n
CCn
FD'n
F'n
Sn
SD'n
FC
GC
An+1
An
SDn
RDn
PP-1
Y

FIG. 7

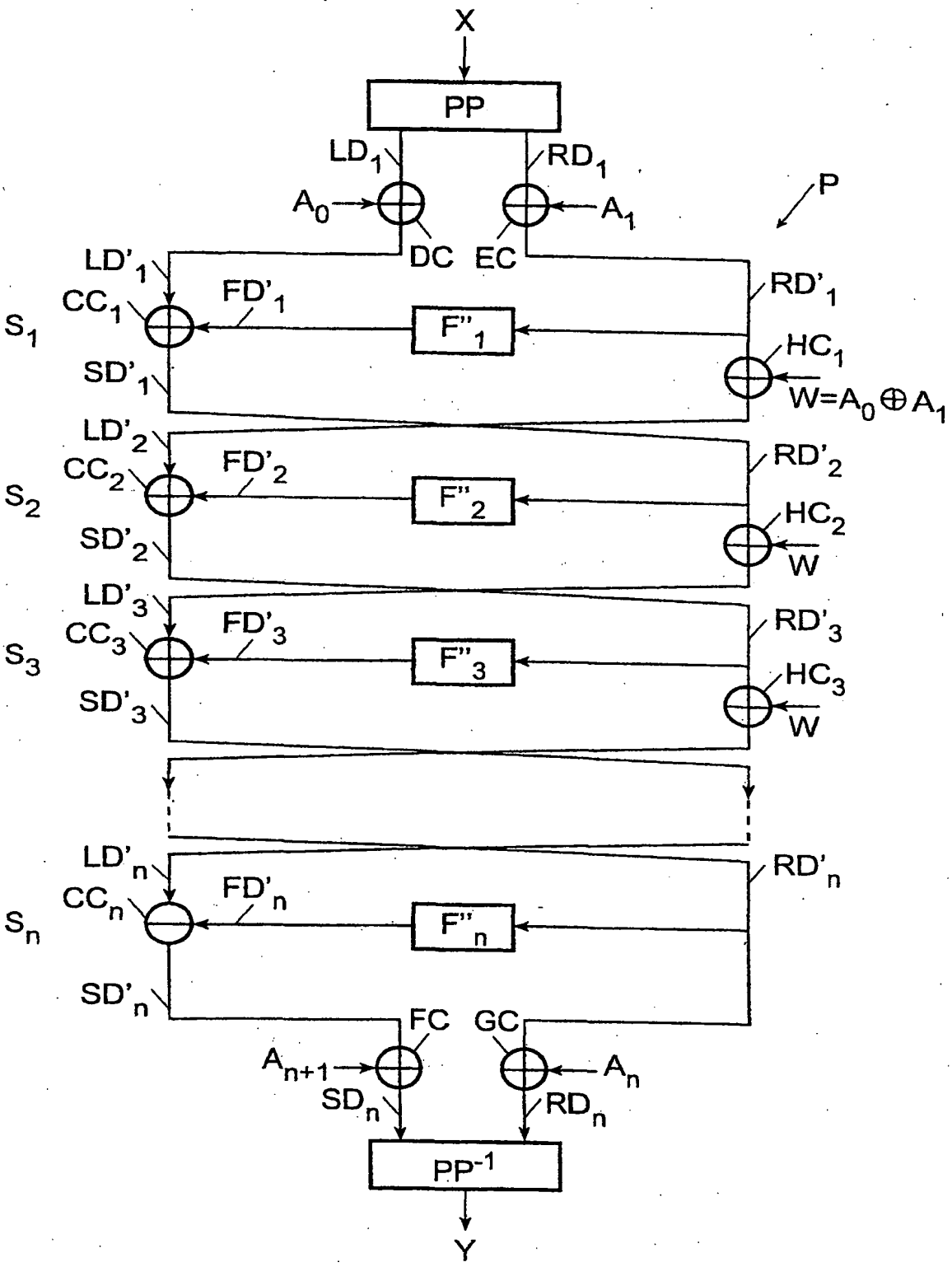

X
PP
LD1
RD1
A0
A1
P
DC
EC
LD'1
CC1
FD'1
F"1
RD'1
S1
HC1
SD'1
W=A0⊕A1
LD'2
CC2
FD'2
F"2
RD'2
S2
HC2
SD'2
W
LD'3
CC3
FD'3
F"3
RD'3
S3
HC3
SD'3
W
LD'n
CCn
FD'n
F"n
RD'n
Sn
SD'n
FC
GC
An+1
An
SDn
RDn
PP-1
Y

FIG. 8

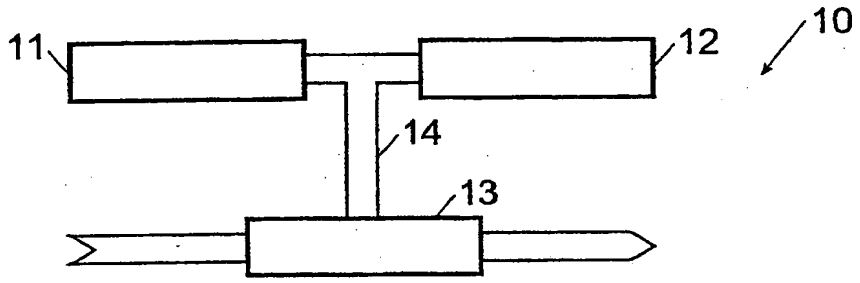


FIG. 9

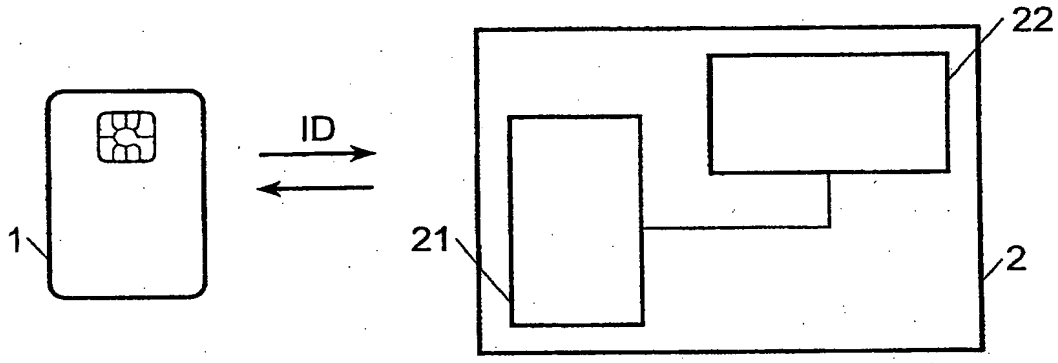


FIG. 10

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/EP 99/10208

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 5 745 577 A (LEECH MARCUS D) 28 April 1998 (1998-04-28) abstract column 2, line 55 -column 3, line 46 column 5, line 6 -column 6, line 4 claims 1,6,7 figures 5,6,8,9	1,2,7,8, 21-23 3-6,9, 10,13
P,X	EP 0 896 452 A (HITACHI LTD) 10 February 1999 (1999-02-10) abstract page 2, line 54 -page 3, line 25 page 9, line 8 - line 46 claim 1 figure 13	1-3, 21-23

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 April 2000	10/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Gautier, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/EP 99/10208

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 724 428 A (RIVEST RONALD L) 3 March 1998 (1998-03-03) abstract column 5, line 65 -column 6, line 50 figures 1B,2	1,2,8, 21,22

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern al Application No
PCT/EP 99/10208

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5745577 A	28-04-1998	NONE	
EP 0896452 A	10-02-1999	JP 11109853 A	23-04-1999
US 5724428 A	03-03-1998	US 5835600 A	10-11-1998